Bridge CA Interoperability Demonstration-Technical Overview

Presentation to the FPKI TWG
8 September 1999

David Lemire
A&N Associates

Topics

- Technical Interoperability Profile
- Certificate & CRL Profiles
- Demonstration Structure
  - Network View
  - PKI View
- Scenarios

Technical Interoperability Profile

- Used To Document Implementation Agreements:
  - Based On Commercial Standards and Practices
  - Assumes Reuse of Existing Applications and Infrastructure Components
- Goals:
  - Specify Details Required for Interoperability
  - Share Information to Avoid Non-Interoperability
- Didn't Want to Over Specify

TIP Document

- Evolved Over Course of Demonstration Effort
- Outline:
  - Introduction
  - Reference Documents
  - Simplifying Assumptions
  - Cryptographic Algorithms
  - Communications Protocols
  - Certificate and CRL Profiles (Booz· Allen)
  - Directory Schema and Protocols (Chromatix)

Reference Documents

- Mail RFCs: SMTP, POP3, MIME, PKIX
- S/MIMEv3 Internet Drafts
- LDAP v2 and v3 RFCs
- X.500 recommendations (1993)
- X.509 recommendations (1993)
- SDN.706 – MISSI Certificate & CRL Profile
- SDN.604 – MISSI Algorithms Implementations

Simplifying Assumptions

- Exchange of Cross-certificates on Magnetic Media
- No Use of Certificate Enrollment Protocols
- Direct Creation and Initial Population of Directory Entries by DSA Administrators
- Single Certificate Policy Throughout Demonstration

TIP Overview

- Key Management: **RSA**
- Signature: **RSA**
  - May Implement **DSA** in Later Phases
- Hash/Digest: **MD5**
- Security Protocol: **S/MIMEv3 CMS/ESS**
- Certificate Path Processing:
  - DOD Applications: **SDN.706-Based Approach**
  - Entrust Applications: **Entrust Approach**

TIP Overview

- Certificate Path Navigation:
  - DOD Applications: **Cygnacom Approach**
  - Entrust Applications: **Entrust Approach**
- Directory:
  - DOD: **Chromatix SafePages w/ LDAPv3 and X.500 DAP**
  - Entrust: **Entrust-Selected w/LDAPv3**
- Directory Schema: **LDAPv2-based**
- DSA-DSA Interactions: **X.500 DSP (1993)**
- Access Control: None in Phase 1

Communications Protocols

Action	Interface	Protocol
Transmit message	Messaging Client to SMTP/POP Server	RFC 822/MIME message, containing CMS/ESS objects, transmitted via SMTP
Retrieve message	Messaging Client to SMTP/POP Server	RFC 822/MIME message, containing CMS/ESS objects, retrieved via POP3
Post Certificate or CRL	Any CA to DSA	LDAPv3 or X.500 DAP
Retrieve Certificate or CRL	Messaging Client to DSA	LDAPv3 or X.500 DAP
Directory request chaining	DSA to DSA	X.500 DSP
Issue certificate to subordinate CA or end-entity (DOD side)	CA to LYNKS Card	Direct physical connection for LYNKS card programming, Sneakernet transfer to card recipient
Exchange of public keys for cross-certification	Principal CAs to BCA BCA to Principal CAs	Self-signed certificates on 3-1/2" floppy disk, with the certificates formatted in accordance with the appropriate profile.
Create and populate directory entries	DSA Administrator to DSA	Direct action at DSA console

Certificate & CRL Profiles

- Minimum Certificate and CRL profile
  - Minimum=
    - Specify Minimum Amount Required for Interoperability
    - Allow CAs to Fit to CA and EE Needs As Appropriate
    - Total Length: 4 Pages
- Standards Compliant
  - Compliant With the X.509 Profile
  - Compliant With PKIX Profile
- All Entity Profiles Are in Agreement With This Profile Unless Otherwise Noted
- Formulated by Booz· Allen & Hamilton

Minimum Certificate Profile Example 1: Base Certificate

Field Name	Usage	Notes
(U)		
version	r	
serialNumber	r	
signature	r	
Algorithm	r	RSA with MD5 OID: 1.2.840.113549.1.1.4
Parameters	r	Null for RSA/MD5.
issuer	r	printableString
validity	r	
notBefore	r	UTC Time
notAfter	r	UTC Time
subject	r	printableString; DN must always be present.
subjectPublicKeyInfo	r	
Algorithm	r	RSA OID: 1.2.840.113549.1.1.1
Parameters	r	Null for RSA.
subjectPublicKey	r	Subject's public key
issuer Unique Identifier	x	Prohibited.
subject Unique Identifier	x	Prohibited.
extensions	r	Profiled in Section 3.

Minimum Certificate Profile Example 2: Extensions (Subset)

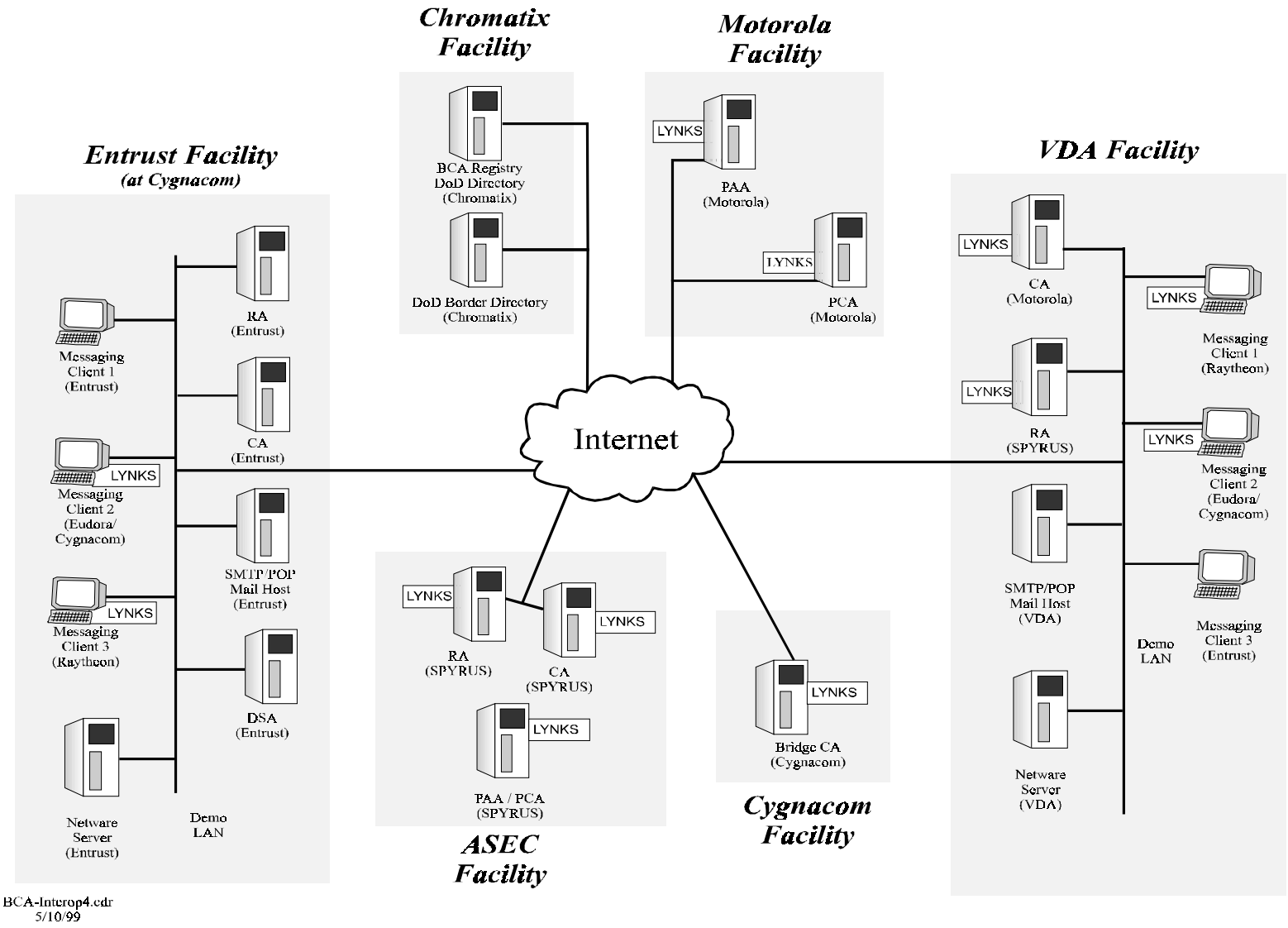
Extension Fields	Usage	Notes
(U)		
authorityKeyIdentifier	r	Required to build certificate path.
keyIdentifier	r	
authorityCertIssuer	-	This field is not used.
authorityCertSerialNumber	-	This field is not used.
subjectKeyIdentifier	r	Required to build certificate path.
keyUsage	k, r	Limit usage to digitalSignature, keyCertSign and cRLSign
extendedKeyUsage	o	Demontration does not make use of this field. If this extension is used, it should not be marked critical.
privateKeyUsagePeriod	o	No trusted time stamping mechanism. If this extension is used, it should not be marked critical.

Minimum CRL Profile - Example: CRL Extensions (Subset)

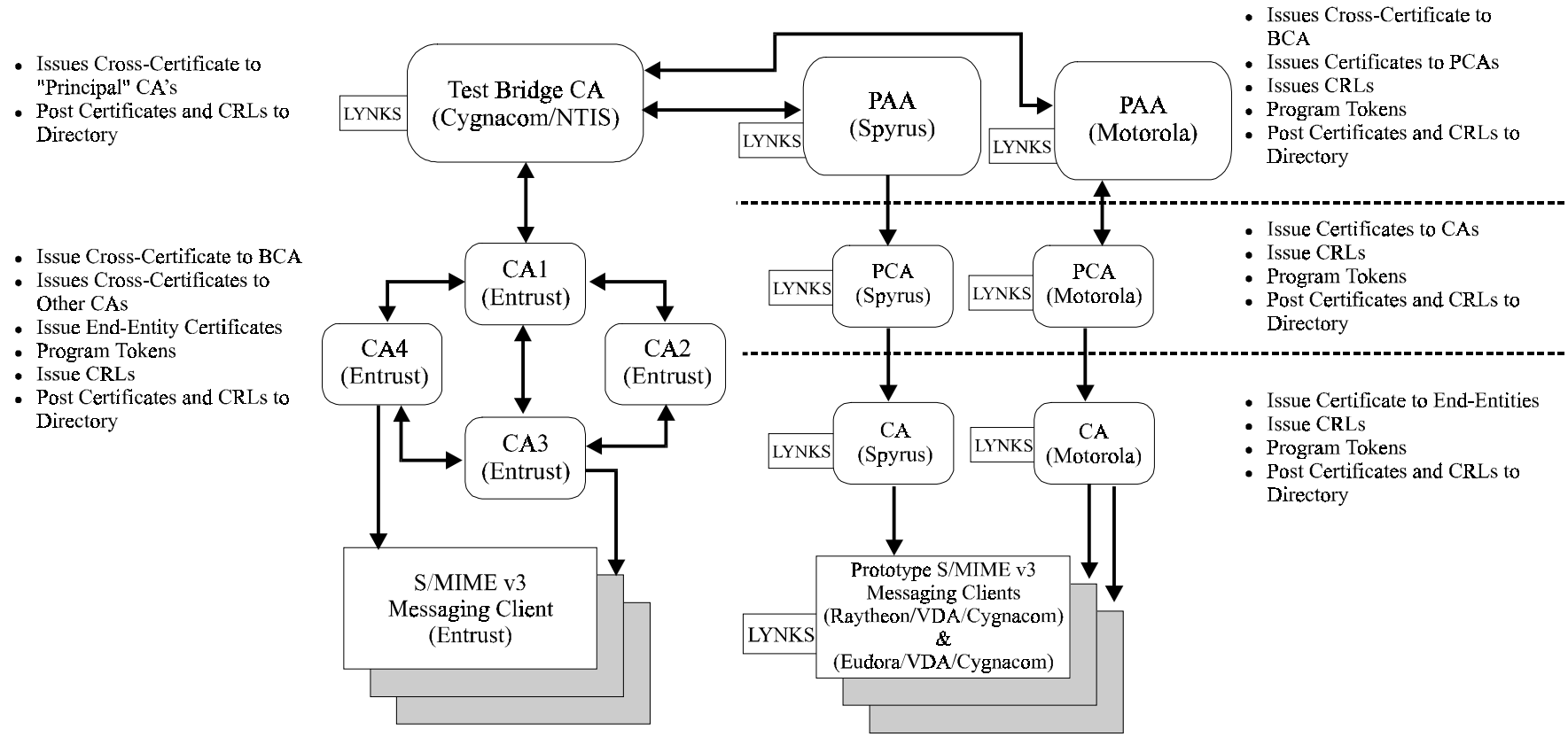
Field Name	Usage	Notes
(U)		
authorityKeyIdentifier	r	
keyIdentifier	r	
authorityCertIssuer	-	This field is not used for the demonstration, but at the same time is not prohibited from being populated by a CA.
authorityCertSerialNumber	-	This field is not used, but at the same time is not prohibited from being populated by a CA.
issuerAltName	o	Demonstration does not make use of alternate names.

A&N Associates, Inc.

Network View



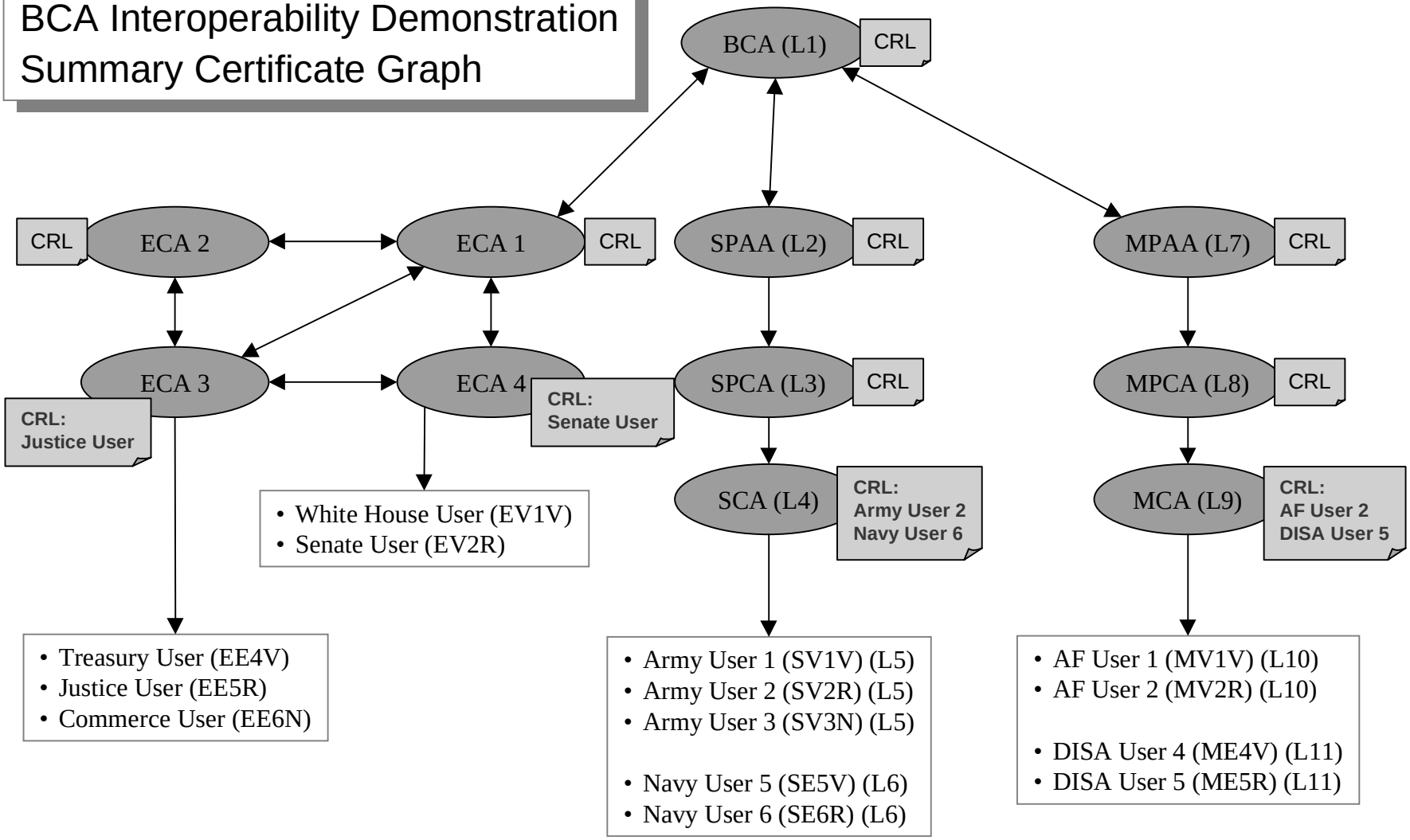
PKI View


Issues Cross-Certificate to "Principal" CA's
Post Certificates and CRLs to Directory
Test Bridge CA (Cygnacom/NTIS)
LYNKS
PAA (Spyrus)
LYNKS
PAA (Motorola)
LYNKS
Issues Cross-Certificate to BCA
Issues Certificates to PCAs
Issues CRLs
Program Tokens
Post Certificates and CRLs to Directory
Issue Cross-Certificate to BCA
Issues Cross-Certificates to Other CAs
Issue End-Entity Certificates
Program Tokens
Issue CRLs
Post Certificates and CRLs to Directory
CA1 (Entrust)
CA4 (Entrust)
CA2 (Entrust)
CA3 (Entrust)
PCA (Spyrus)
LYNKS
PCA (Motorola)
LYNKS
Issue Certificates to CAs
Issue CRLs
Program Tokens
Post Certificates and CRLs to Directory
CA (Spyrus)
LYNKS
CA (Motorola)
LYNKS
Issue Certificate to End-Entities
Issue CRLs
Program Tokens
Post Certificates and CRLs to Directory
S/MIME v3 Messaging Client (Entrust)
Prototype S/MIME v3 Messaging Clients (Raytheon/VDA/Cygnacom) & (Eudora/VDA/Cygnacom)
LYNKS

Demonstration Scenarios

- Messaging Oriented Scenarios
  - Certification Path Construction
  - Revocation Checking
  - 3 PKIs, 3 Client Types
- Border Directory Scenario
  - Directory Browsing
  - Entry Visibility/Invisibility

BCA Interoperability Demonstration Summary Certificate Graph



Messaging Scenario 1

- Purpose: Navigate Certification Paths Through BCA
- Approach: Messages Across Each PKI Pair Using Variety of Clients

Seq. Num.	PKIs	Clients	Specific Message Flows
1	SPYRUS → Entrust	→ Entrust	Navy User 5 (SE5V) → Treasury User (EE4V)
2	SPYRUS → Motorola		Navy User 5 (SE5V) → DISA User 4 (ME4V)
3	Motorola → Entrust	→ Entrust	DISA User 4 (ME4V) → Treasury User (EE4V)
4	Motorola → SPYRUS		DISA User 4 (ME4V) → Navy User 5 (SE5V)
5	Entrust → SPYRUS	Entrust →	Treasury User (EE4V) → Navy User 5 (SE5V)
6	Entrust → Motorola	Entrust →	Treasury User (EE4V) → DISA User 4 (ME4V)

Messaging Scenario 2

- Purpose: Process Revocation on Certification Paths Through BCA
- Approach: Process Messages from Revoked EEs under "Foreign" PKIs

Seq. Num.	PKIs	Clients	Specific Message Flows
1	SPYRUS → Entrust	→ Entrust	Navy User 6 (SE6R) → Treasury User (EE4V) — **FAILS**
2	Entrust → Motorola	Entrust →	Justice User (EE5R) → DISA User 4 (ME4V) — **FAILS**
3	Motorola → SPYRUS	→	DISA User 5 (ME5R) → Navy User 5 (SE5V) — **FAILS**

Messaging Scenario 3

- Purpose: Participation of New EEs in Larger Community
- Approach: Create New EE and Originate Messages

Seq. Num.	PKIs	Clients	Specific Message Flows
1	Entrust → SPYRUS	Entrust →	Commerce User (EE6N) → Navy User 5 (SE5V)
2	Entrust → Motorola	Entrust →	Commerce User (EE6N) → DISA User 4 (ME4V)
3	SPYRUS → Entrust	→ Entrust	Navy User 5 (SE5V) → Commerce User (EE6N)
4	Motorola → Entrust	→ Entrust	DISA User 4 (ME4V) → Commerce User (EE6N)

Messaging Scenario 4

- Purpose: Effects of Revoking a Principal CA
- Approach:
  - Revoke one Principal CA
  - Demonstrate Message Flow in Both Direction

Seq. Num.	PKIs	Clients	Specific Message Flows
1	Motorola → Entrust	→ Entrust	DISA User 4 (ME4V) → Treasury User (EE4V) — **FAILS**
2	Motorola → SPYRUS	→	DISA User 4 (ME4V) → Navy User 5 (SE5V) — **FAILS**
3	SPYRUS → Entrust	→ Entrust	Navy User 5 (SE5V) → Treasury User (EE4V)
4	SPYRUS → Motorola	→	Navy User 5 (SE5V) → DISA User 4 (ME4V)
5	Entrust → SPYRUS	Entrust →	Treasury User (EE4V) → Navy User 5 (SE5V)
6	Entrust → Motorola	Entrust →	Treasury User (EE4V) → DISA User 4 (ME4V)

Summary . . .

- TIP
  - Used to Document Technical Agreements
    - Emphasis on Commercial Standards
    - Emphasis on Reuse of Existing Products
  - Basis for Current (Phase 1) Demonstration
  - Can Be Extended if Demonstration Extended
- Networks and Facilities
  - Two Primary Demonstration Facilities
  - Several Support Facilities
  - Internet Employed As Underlying WAN

. . . Summary

- PKIs
  - Three PKIs Connected Through Pilot BCA
  - Two Hierarchies, One Mesh
  - Based on Existing Products & Standards
- Scenarios
  - Messaging
    - Demonstrate Interoperability and Revocation
  - Border Directory
    - Demonstrates Private / Public Directory Separation